MFE-IT

Reference: MB/EN/SEC1

Cybersecurity Best Practices Training Course

Identifying Threats and Reducing Risks in Your Organisation

Duration: 2 Days | Hours: 12 h

Remote · Sessions guaranteed from 1 registrant · 60% hands-on practice

DESCRIPTION

Phishing, ransomware, data leaks, account compromise — cyber threats are on the rise and now affect organisations of every size. Awareness and a clear understanding of the risks are essential across all professions, not just IT teams.

This cybersecurity training course offers a clear, practical and accessible approach to identifying threats, recognising risky behaviours, applying everyday best practices and reacting effectively when an incident occurs. The objective is to build a sustainable security culture within the organisation, with concrete reflexes that every employee can apply from day one.

LEARNING OBJECTIVES

By the end of this training course, participants will be able to:

- Understand the main types of IT threats (malware, phishing, DDoS attacks)
- Identify human, technical and organisational vulnerabilities
- Assess the organisation's exposure to digital risks
- Apply best practices in security (authentication, passwords, updates, email)
- Know how to respond in the event of an incident or suspected attack
- Promote a culture of security within the organisation

PREREQUISITES

- No technical prerequisites required
- Curiosity and interest in current digital issues

> *Because each participant is unique, a personalised interview is systematically organised in advance with our expert to design a training programme perfectly aligned with their objectives, level and professional challenges.*

TARGET AUDIENCE

Employees, technical teams and business managers who wish to strengthen the company's overall security posture.

DETAILED PROGRAMME

> The training alternates between theoretical input and hands-on practice (approximately 60% of the time). Modules are built around practical exercises based on real-world business use cases.

Module 1 – Overview of Current Threats

- Types of attacks: phishing, ransomware, spyware, brute force
- Account compromise and shadow IT
- Real-world incident examples and impact

Module 2 – Risks and Vulnerabilities in Business

- Technical risks: obsolete software, open ports, misconfigurations
- Human risks: behaviour, errors and social engineering
- Organisational risks and weak security governance

Module 3 – Good Security Practices

- Strong authentication and password management
- Mobile and Wi-Fi security
- Software updates and reliable backup strategies

Module 4 – Responding to a Threat

- Recognising a phishing attempt
- What to do in case of intrusion or suspicious activity
- Who to alert and the first steps to take

Module 5 – Awareness and Proactive Approach

- Integrating security into everyday practices
- Everyone's role in cybersecurity
- Long-term prevention and security culture

TEACHING METHODS

Format and Delivery

The training is delivered remotely via an interactive virtual classroom. It can also be delivered on-site, with content customised to match the needs of your professional project. The theory/practice split is approximately 40%/60%.

MFE-IT Ultra-Personalised Format

Each session accommodates between 1 and 3 participants, ensuring highly individualised support. A preliminary interview allows us to tailor the content to each participant's profile. Inter-company sessions are guaranteed from just 1 registrant (except in cases of force majeure).

Skills Assessment

Throughout the training, the trainer assesses participant progress through multiple-choice questions, role-playing exercises and hands-on work. At the end, a certificate of achievement is issued to each participant.

Post-Training Support

For one month following the training, each participant can contact MFE-IT trainers with questions about implementing acquired knowledge. A response is provided by email or telephone within 48 working hours.

Accessibility

MFE-IT is committed to welcoming people with disabilities. Contact: contact@mfe-it.com.

PRACTICAL INFORMATION

Trainer Resources

- Structured demonstrations aligned with the detailed programme
- Exercise briefs and solutions throughout the training
- A ready-to-use technical environment for practical workshops
- Trainer validation of acquired knowledge at the end of each workshop
- Digital reference documents

Certification and Validation

At the end of the training, a certificate is sent by email specifying the objectives, nature, duration and assessment results. A completion certificate can also be provided on request.

Benefits for Participants

- Train from your workplace or home, with no travel required
- Benefit from an expert trainer-consultant on the subject
- Enjoy an ultra-personalised format (1 to 3 participants)
- Continue training even in the event of unforeseen circumstances

Benefits for the Organisation

- Optimise the training budget by reducing travel and accommodation costs
- Offer quality training to all employees, regardless of location
- Reduce absence time linked to travel
- Support team upskilling in all contexts